Journal of KONBiN 3(35)2015
ISSN 1895-8281
DOI 10.1515/jok-2015-0048 ESSN 2083-4608

# SELECTED METHODS FOR INCREASES RELIABILITY THE OF ELECTRONIC SYSTEMS SECURITY

# WYBRANE METODY ZWIĘKSZENIA NIEZAWODNOŚCI W ELEKTRONICZNYCH SYSTEMACH BEZPIECZEŃSTWA

**Jacek Paś**

Wojskowa Akademia Techniczna
*e-mail: jpas@wat.edu.pl*

***Abstract****: The article presents the issues related to the different methods to increase the reliability of electronic security systems (ESS) for example, a fire alarm system (SSP). Reliability of the SSP in the descriptive sense is a property preservation capacity to implement the preset function (e.g. protection: fire airport, the port, logistics base, etc.), at a certain time and under certain conditions, e.g. Environmental, despite the possible non-compliance by a specific subset of elements this system. Analyzing the available literature on the ESS-SSP is not available studies on methods to increase the reliability (several works similar topics but moving with respect to the burglary and robbery (Intrusion.) Based on the analysis of the set of all paths in the system suitability of the SSP for the scenario mentioned elements fire events (device) critical because of security.*

***Keywords:*** *electronic security, redundancy of, reliability, power*

***Streszczenie:*** *W artykule przedstawiono zagadnienia związane z wybranymi metodami zwiększenia niezawodności w elektronicznych systemach bezpieczeństwa (ESB) na przykładzie systemu sygnalizacji pożarowej (SSP). Niezawodność SSP w sensie opisowym to własność zachowania zdolności do realizacji zadanych funkcji (np. ochrona: przeciwpożarowa lotniska, portu, bazy logistycznej, itd.), w określonym czasie i w określonych warunkach np. środowiskowych, pomimo ewentualnego niespełnienia wymagań przez określony podzbiór elementów tego systemu. Analizując dostępną literaturę na temat ESB-SSP brak jest dostępnych opracowań na temat metod zwiększenia niezawodności (kilka prac poruszających podobne tematy ale odniesieniu do systemów sygnalizacji włamania i napadu (SSW i N). Na podstawie przeprowadzonej analizy zbioru wszystkich ścieżek zdatności w systemie SSP dla przyjętego scenariusza zdarzeń pożarowych wskazano elementy(urządzenia) krytyczne ze względu bezpieczeństwo. Wskazano metody zwiększenia niezawodności dla rozpatrywanego systemu.*

***Słowa kluczowe:*** *elektroniczne systemy bezpieczeństwa, nadmiarowość, niezawodność, zasilanie*

## 1. Introduction

Reliability of electronic security system in a descriptive sense is a property preservation capacity to implement the preset function (eg. security against: fire or building, port, database burglary, etc.), at a certain time and under certain conditions (eg. Environmental I - IV according to the standard PN EN-50131-1: 2009), in spite of a possible failure to meet the requirements for a specific subset of the system's elements. ESS electronic security system is a separate entity from the environment (eg. A system intrusion SSW and N, integrated fire alarm system SSP, etc.) working, due to the synergistic interaction of its existing components (eg. The detector (s) - the control panel - the transmission line - Actuator - smoke damper-hydraulic cylinder). ESB is a set of the interacting elements that are deliberately integrated in order to ensure safety e.g. against fire [2,3]. The definition of ESB can be written according to the following formula:

$$\mathbf{S_{ESB} = [E; W; R]} \quad (1)$$

where:
ESB - ESB system matrix,
E - vector elements of the ESB,
W - properties vector of the individual ESB elements,
R - relationship transfer vector (flow) or call (control, stabilization) between ESB system components (eg. the detector - the control panel, headquarters - execution system).

Relationship between the different parts of the ESS system can be either direct or indirect (direct - a combination of sensors via bus transmission to the control panel, indirect- manual fire alarm activation and commissioning ROP control ventilation or fire separations.). Moreover, relationships between different elements of the ESS system can be linear or nonlinear. ESB reliability can be defined as an ability to maintain system's readiness in order to secure the implementation of the assumed functions - eg. firefighting scenario - Fig. 2. safety ensuring of the ESB system is to counteract the protected objects three processes - Fig. 1.

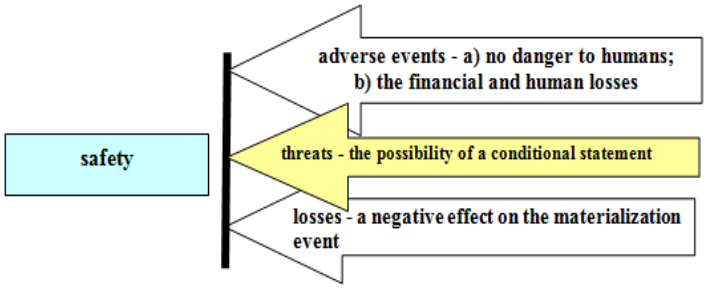


*Fig. 1 The concept of security in electronic security systems [own work]*

Special requirements apply to technical and operational SSP systems. SSP systems according to PN-CEN / TS EN 54-14 points. 14 is a hierarchical system - used in places where the guarded object is divided into a number of smaller parts [1,2].

In large (wide-area) savings buildings in their wiring can be installed slave control panels (CA), which carry out their hindquarters and at the same time communicate with the parent panel.

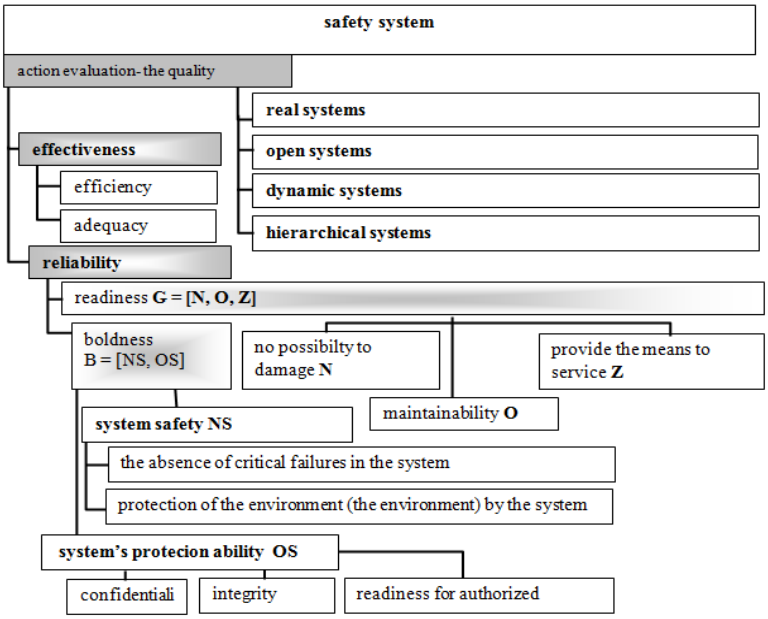


*Fig. 2 Basic concepts relating to the operation of electronic security systems process [own study based on 1,3]*

## 2. Basic assumptions about the reliability of the elements (devices) that create the SSP

SSP is a complex technical systems containing both electronic components (devices) - sensors, power modules, etc. and mechanical components - motors, valves, etc. [1,2,4,5]. In the security system, in which there are redundant components, can be distinguished minimum suitability track or minimum unsuitability dimensions [5,6,8]. In relation to security systems without reserve in systems, where there are elements of the reserve ,there are at least two fitness paths (in the case of reserving one additional element, or n - paths in case of n - reserve elements).

Minimum security system fitness path $S_{ZSB}$ - we call it minimal subset of the safety components (in the path also includes system elements forming a structural surplus), which found itself in a position to cause the overall security system suitability - Figure 3.

Minimum cross $S_{NSB}$ unfitness security system - called a minimal subset of system components (including system components forming the structural surplus), which found itself unable to make it unfit to the overall security system [10,11,12].

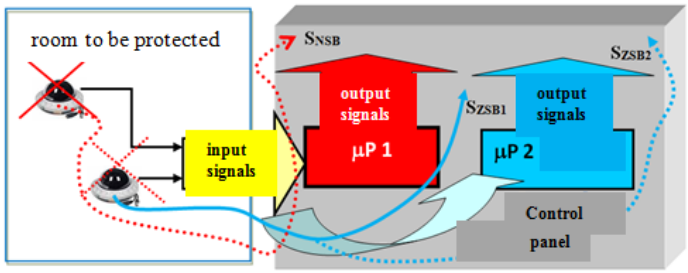


*Fig. 3 SSP fitness paths, taking into account the structural surplus [own work]*

Fitness path $S_{ZSB}$ SSP system can be regarded as a system with a serial structure. Reliability and the minimum fitness path of system's safety can be determined from the following formula:

$$P(B) = 1 - \sum_{i=1}^{N} q_i + \sum_{i<j} q_{ij} + \ldots + (-1)^{N-1} q_{1,2,\ldots,N} \tag{2}$$

where:

B - consisting of the event that there has been no security risk of the system (safety system capable of implementing functions);
P(B) - security;
N - number of elements of the safety system, i = 1,2, ..., N;

$$q_i = P(\overline{A}_i) \tag{3}$$

- an event consisting in the fact that the i- th element of the security system does not meet the requirements;
- an event consisting in the fact that the i – th element of the safety system meets the requirements;

$$q_{ij} = P(\overline{A}_i \bigcap \overline{A}_j) \tag{4}$$

- an event consisting in the fact that the j - th element of the security system does not meet the requirements. All the suitability of the system consists of a path parallel system.

## 3. The fire scenarios for a complex system SSP

Polish law requires fire scenario development, tailored to the individual structure. This obligation is defined in the Regulation of the Minister of Internal Affairs and Administration of 16 June 2003. Scenario of events during a fire, or a basic scenario that requires us to prepare the Polish law, depending on the needs of the investment can be enhanced with additional steps, which contain a more detailed content:

– scenario-algorithms (description of the installation and any equipment when the fire starts);
– scenario-matrix (program all the anti-fire devices with descriptions of their interactions controls needed for fire equipment.);
– scenario post-completion (needed for operation of the facility) [1,3].

Due to the two-stage fire alarm organization, fire alarm degree (e.g. Pre-alarm) can be triggered by a signal from a fire detector installed in the facility. In the absence of personnel response and the degree of alarm after 30 seconds the alarm changes to alarm the second degree, and is activated by a procedure associated with object's fire protection. Secondary fire alarm can be triggered by a signal from a single detector and automatic control switch into alarm the second degree after diagnosis time (T2), or until it is confirmed (T1). Detectors coincidence located in alarm system which are independent in technical terms and due to their reliability, are connected to the transmission bus with individual addressing and internal short circuit isolators [7,13]. SSP complex system diagram is shown in Fig. 5. The system consists of a control panel that controls the various subsystems - gas extinguishing systems, sprinklers and sprinkler system, conventional SSP deployed in the works 1-n, the system alarm signals with acoustic-signaling system optic. The control panel also oversees control actuators through fire separations, elevators, flaps and actuators e.g. ventilation flaps (shown in Fig. 5.). The fire protection supervisory system SSP is presented in an extensive construction work which includes a mind map - fire scenario. The paper presents the possibility of a limited number of fire spread scenarios and limited amount of system components for cases 1-4, and also the possibility of so-called block fire (fire covering several building's tiers or group of buildings) in the absence of response to such an internal fire or the possibility of hidden fire (fire in the empty ceilings spaces, walls without signs of light and glow) or open (fire in a confined space as above, but with visible fire ) [12,13,14].

## 4. The selected track system SZS SSP suitability for the situation with the fire scenario

Depending on the fire scenario (Fig. 6) for illustrated in Fig. 5 SSP system can distinguish different paths for existing so-called fitness, e.g. 'partial' or 'limited' fire including a separate area (s) of the building - $S_{ZS1}$, $S_{ZS2}$, ..., and the block fire $S_{ZS}$. In the case of restricted fire only the part of the SSP system equipment (components) is involved in the fire action.
When the block fire occurs then all devices (elements) are taking part in the fire. In Fig. 7, 8 is presented a diagram of the path for the system's suitability for limited fire SSP, while Fig. 9 presented a schematic scenario in the event of block fire.
For the fitness path 2 $R_{zn}2$ reliability function (t) can be estimated according to the formula 4. The reliability $R_{zn}2$ (t) is a conditional function because the alarm signal is generated in response provided at least two detectors for simultaneously alerting group in Group A, Zone 1 (Fig. 4). For fire scenario 3 (internal fire - open) $R_{zn3}$ reliability function (t) can be estimated by the formula 5 while a simplified diagram for estimating the reliability function for the track number 3 is shown in Fig. 8.
$R_{zn3}$ reliability function (t) is also a conditional function because the alarm signal is generated in response provided at least two detectors for simultaneously alerting ROP group or sensor - manual fire alarm. In this case, the CA implements established scenario - matrix controls ,e.g. program of all fire equipment together with descriptions of their interactions needed for fire equipment controls. Fig. 9 shows a simplified diagram for estimating the reliability function in event of block fire scenario.

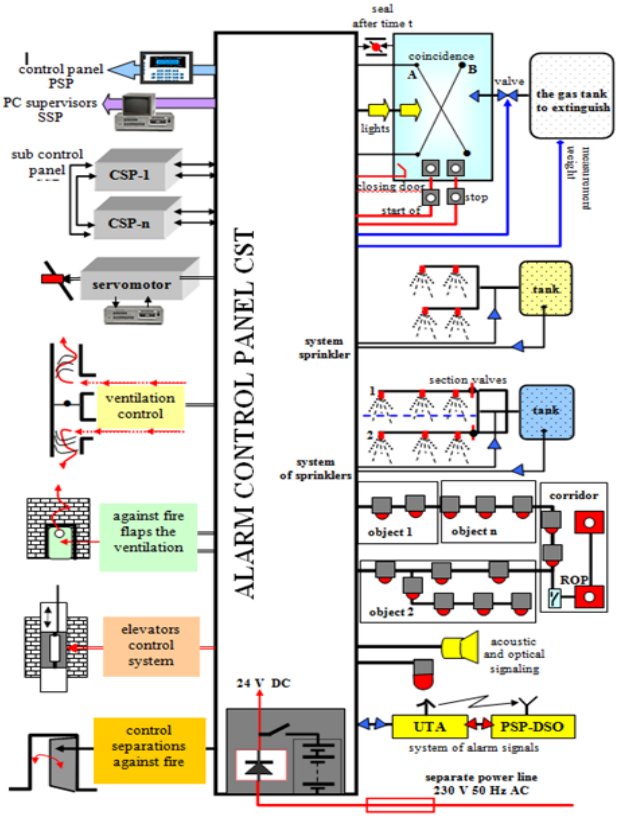


*Fig. 5 Technical Complex fire alarm system [own study based on 1,2,3]*

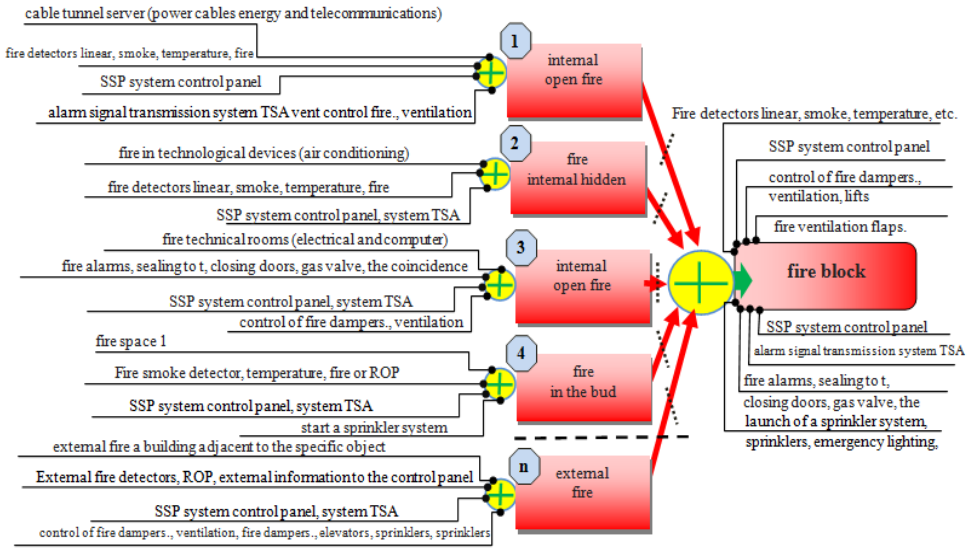


*Fig. 6 A mind map - the fire scenario shown in Fig. 5. System [own work]*

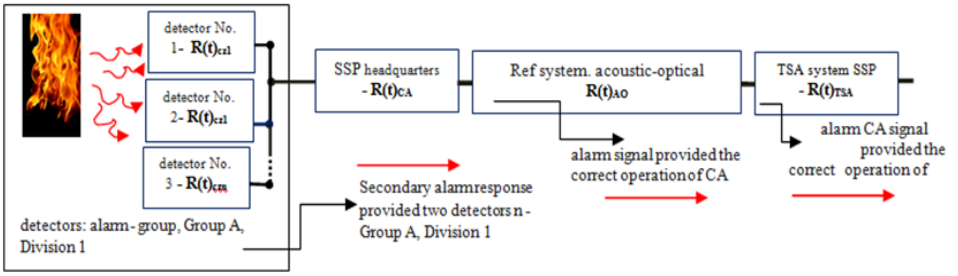


*Fig. 7 Simplified diagram for estimating the reliability function for the path No. 1 fire scenario [own work]*

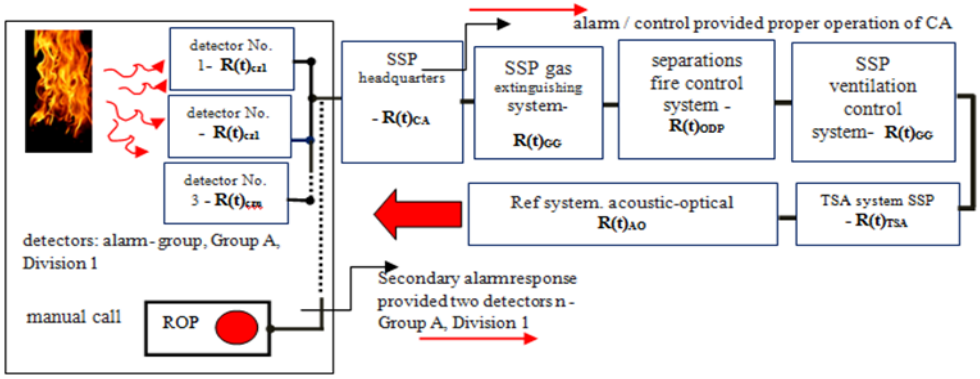


*Fig. 8 Simplified diagram for estimating the reliability function for the path No. 2 fire scenario [own work]*

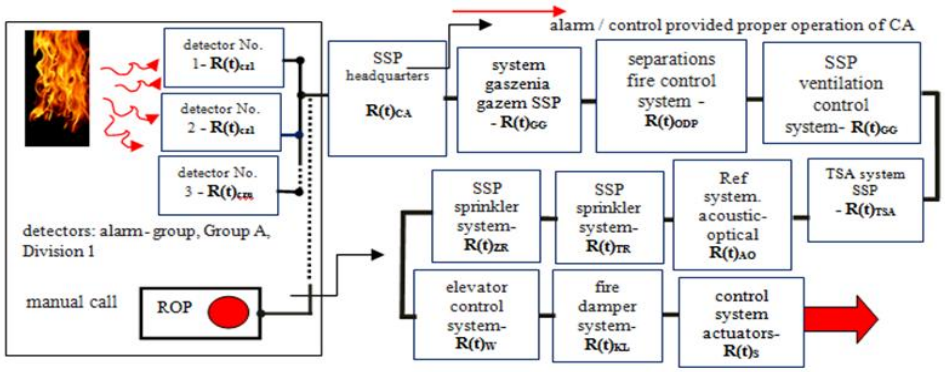


*Fig. 9 Simplified diagram for estimating the reliability function for block fire scenario [own work]*

## 5. Decentralized control fire alarm system

Shown in Fig. 7-9 simplified diagrams for estimating the reliability function for fire scenario shown in Fig. 6 are mixed reliability structure, series - parallel. Ordered and parallel structure exists only in the group of detectors for

simultaneously alerting group in Group A. The implementation of this function is reserved for the second degree alert alarm without the roger fire by fire service system. In this case, two counting detectors must confirm the fire presence. In the event of MCP activation system automatically generates a second degree alert signal, without using acknowledgment of this signal. Shown in Fig. 7 - 9 reliability diagrams for different fire scenarios in addition to the notification function form (detector) serial reliability structure. In this structure, the stability of the resultant object (system) is determined by the stability of the SSP weakest equipment item. As shown in Fig. 7 - 9 simplified schemes for estimating the reliability function for selected fire risk scenarios, the element that determines the adoption, implementation and control of all fire equipment is connected in a defined system control panel decides [8,9,10]. If any damage occurs to the SSP system's control panel, the system is not able to properly perform its function. Therefore, the matrix controls and developed scenarios of fire, follow the decentralization system controls, implementing these features through the expander alarm [8,10,14]. In this case, all normal damage to a single panel is the lack of implementation of the fire only a single function - eg. start smoke dampers. The realization of the control system, alarm at control panels SSP shown in Fig. 10. Each expander panels perform specialized functions of control, as well as, answering common area surveillance in the facility, including the diagnosis.

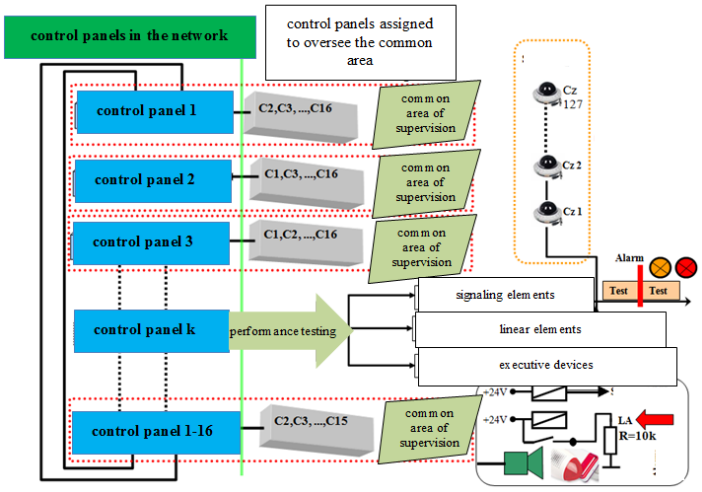


*Fig. 10 The reliability increase of the SSP by using a expander C1-C16 [own work]*

## 6. Conclusions

Developing optimal fire scenario and matrix system for complex controls fire is a very complex issue.

Achieving all the tactical and technical SSP system, including a predetermined level (value) of the function in a complex system reliability SSP is a difficult issue in the practical implementation [6,9]. Due to the use and implementation of security features (eg. human life, property, tangible or intangible value, etc.) SSP systems cannot be integrated with other alarm systems (eg. SSWiN, SKD, CCTV) found in the premises [4,6,8,10]. Increasing the assumed level of SSP system reliability function is an analysis of the suitability of all tracks $S_{ZS}$ for developed algorithm - fire scenario events and the identification of critical elements (devices) inadequacy of the system which causes a lack of response to the threat of safety - fire. One way of using the safety systems is increase the reliability of the active use of redundancy - eg. elemental, time, information, parametric, etc. This method requires a reliability analysis of the whole SSP system, not only devices (components) but also fire systems (subsystems) co - alarm signal transmission system (min. two independent channels alarm) systems, electricity supply (before the fire and during the fire), water supply system and gas to extinguish, etc. This reliability analysis of integrated systems for the SSP is very complex [5,6,10,12]. A better solution is to use the method of decomposition of the SSP system corresponding to a given fire scenario fitness path $S_{ZS}$ and development (calculation) on the basis of the estimated value of the reliability function. Another solution that can be successfully used in SSP systems is increasing the reliability function of a fault tolerance technique widely used in modern rail traffic control systems.

## 7. Literature


[1] Skiepko E.: Instalacje przeciwpożarowe, Wydawnictwo Medium, Warszawa 2009.

[2] Radziejewski R., Siudalski S.: Ochrona osób i mienia, Wydawnictwo WAT, Warszawa 2013.

[3] Mikulik J.: Wybrane zagadnienia zapewnienia bezpieczeństwa i komfortu w budynkach, Wydawnictwo AGH 2008, Kraków

[4] Paś J., Dąbrowski T.: „Methodology of teaching of diagnosing technical security system with examples of system of signalization of burglary and fire" 4TH International Congress on Technical Diagnostic Olsztyn 09-12.09. 2008 r. str. 140

[5] Dyduch J., Paś J.: Eksploatacja transportowych systemów nadzoru na rozległym obszarze kolejowym, VII Krajowa Konferencja „Diagnostyka Techniczna Urządzeń i Systemów" Diag' 2009 Ustroń

[6] Rosiński A.: Reliability analysis of the electronic protection systems with mixed m–branches reliability structure, Advances in Safety, Reliability and Risk Management, Editors: Berenguer, Grall & Guedes Soares. Taylor & Francis Group, London, UK 2012.

[7] Paś J., Duer S.: Determination of the impact indicators of electromagnetic interferences on computer information systems, Neural Computing & Applications, Vol. 23, Issue: 7-8, Special Issue: SI, 2013, p. 2143-2157.

[8] Rosiński A.: Reliability analysis of the electronic protection systems with mixed – three branches reliability structure, Proc. International Conference European Safety and Reliability ESREL 2009, p. 1637–1641.
[9] Choromański W., Dyduch J., Paś J.: Minimizing the Impact of Electromagnetic Interference Affecting the Steering System of Personal Rapid Transit in the Context of the Competitiveness of the Supply Chain, Archives Of Transport, Polish Academy of Sciences Index 201 901 ISSN 0866-9546 Volume 23, Issue 2, Warsaw 2011
[10] Dyduch J., Paś J., Rosiński A.: Podstawy eksploatacji transportowych systemów elektronicznych. Wydawnictwo Politechniki Radomskiej, Radom 2011.
[11] Siergiejczyk M., Rosiński A.: Reliability analysis of power supply systems for devices used in transport telematic systems. The monograph „Modern Transport Telematics", Communications in Computer and Information Science, Vol. 239. The publisher: Springer-Verlag, Berlin Heidelberg (2011)
[12] Laskowski D., Łubkowki P.: The end-to-end rate adaptation application for real-time video monitoring, Advances in Intelligent Systems and Computing, Springer International Publishing AG, Switzerland, Volume 224, 2013. p. 295-305.
[13] Burdzik R., Konieczny Ł.: Research on structure, propagation and exposure to general vibration in passenger car for different damping parameters, Journal of Vibroengineering Vol. 15, Issue 4, 2013, p. 1680-1688.
[14] Sumiła M., Siergiejczyk M.: Method of dynamic identification of hazardous driver behavior by traffic parameters detection. Safety and Reliability Methodology and Applications – Nowakowski et al. (Eds). CRC Press Taylor & Francis Group. London 2015. p. 109 – 114

***Jacek Paś, PhD Eng.*** *- he defended his doctoral thesis at the Kazimierz Pulaski University of Technology and Humanities in Radom, at the Faculty of Transport and Electrical Engineering, in Poland, in 2010. Currently, he is an assistant professor at the Department of Electronics of the Military University of Technology. His research interests include: electromagnetic compatibility of low frequencies operation, maintenance of electronic safety systems, reliability and maintenance of complex systems.*